

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Peter L. Bergh et al.)	Confirmation # 2348
)	
Application No. 10/605,349)	Examiner: Venkatanaray Perungavoor
)	
Filed: September 24, 2003)	Group Art Unit: 2132
)	
Title: SYSTEM AND METHOD FOR)	
PRESENTATION INTEGRITY)	

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REMARKS IN SUPPORT OF PRE-APPEAL BRIEF REQUEST FOR REVIEW

Applicants submit that the current and preceding office actions issued by the Examiner in the present application contain clear errors in the Examiner's rejections as well as omissions of one or more essential elements needed for a *prima facie* rejection under 35 U.S.C. § 102 and/or 35 U.S.C. § 103.

The present invention is a system and method for ensuring that information content data is presented in the same format to all requestors, clients or viewers. The information content data is capable of being presented in formats other than a predetermined format at different requestors or clients. Formatting data or data used to format the information content data is encrypted to prevent the formatting data from being corrupted or altered. The formatting data is encrypted and decrypted using at least one key or password to prevent the associated information content data from being presented in a format other than the predetermined format at each requestor or client to provide presentation integrity between the different requestors, clients or viewers. In another embodiment of the present invention, the system or method ensures that the proper version of multiple different versions of the content is presented to a particular audience or receiver. This is accomplished by encrypting the formatting data using a key corresponding to the version of the content for the particular audience or receiver.

Claims 1-14, 21-27, 31, 34-36, 40-41, 45-49, 53-56, 59-60, 62-73, 75-82, 85, 90-94, 100, 103-110, 112-114, 132, and 134-141 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Publication 2004/0225891 to Kang et al. (hereinafter Kang). This rejection is respectfully traversed. Turning initially to the rejection of independent claim 1 under 35 U.S.C. § 102(e) as being anticipated by Kang, claim 1 recites:

“an encrypter embodied in a data processing device to encrypt formatting data associated with information content data,”

The Examiner cited FIG. 19 steps S250 and S260 for rejecting this feature of independent claim 1. Kang in FIG. 19 in S250 teaches generating header information and in S260 encrypting the header information. In paragraph [0106] Kang recites the following with respect to the information included in the encrypted header information:

“The header information includes information necessary for encryption of the digital content such as size of the encrypted block, encryption period and encrypted frame unit, etc. The header information is also generated to include the hash value by applying the whole header to the hash algorithm, with which value the change of header information can be determined. The header information generated at the step of S250 is encrypted (S260) and then the information on the encrypted header and the size of the encrypted header is added to the header (S270), so that generated is the header added to the front end of the encrypted digital content transmitted to the user (*sic*).”

Applicant respectfully submits that Kang does not teach or suggest that the header information contains formatting data associated with the content data as required by claim 1.

Additionally, claim 1 recites:

“...wherein the information content data is capable of being presented in a format other than the predetermined format at different requesters or clients, and wherein the formatting data is encrypted and decrypted in response to at least one key or password to prevent the associated information content data from being presented in the format other than the predetermined format at each requester or client to provide presentation integrity between the different requesters or clients.”

The Examiner cited paragraphs [0068], [0076] and [0091] of Kang for rejecting these features of independent claim 1. Applicant respectfully submits that none of these paragraphs teach or suggest the features of the embodiment of the present invention in claim 1 above. Paragraph [0068] of Kang recites:

“The interface 201 receives the key information that has been generated by service server 210 in dependence upon the user's identity characters. User authorization identifier 202 obtains the user's key after reading the header of the copyright protection protocol received from service server 210, and then determines whether the user is authorized to receive digital information by analyzing the user's authorization information with the user's key that has been generated. Temporary validation key decryptor 203 decrypts the temporary validation key by using the user's key provided by user authorization identifier 202. Digital content decryptor 204 decrypts the encrypted digital information received with the copyright protection protocol by using the temporary validation key decrypted by temporary validation key decryptor 203.”

Accordingly, this paragraph of Kang is concerned with determining whether the user is authorized to receive digital information by analyzing the user's authorization information with the user's key that has been generated and in decrypting the encrypted digital information with the copyright protection protocol. This paragraph of Kang does not teach or suggest encrypting the formatting data to prevent the associated information content data from being presented in a format other than the predetermined format at each requestor or client to provide presentation integrity between the different requestors or clients as provided by the embodiment of the present invention as recited in claim 1 above.

Kang in paragraph [0076] describes how user validation keys are generated. Beginning at line 15 of paragraph [0076], Kang recites:

“The user's authorization information furnished by generator 215 is applied to header generator 216, which adds the user authorization information to the header and then provides the header to protocol format generator 217. Protocol format generator 217 forms the copyright protection protocol format by adding the encrypted digital information to the header and then transmits the copyright protection protocol to the user's terminal unit 200.”

Again, Kang is only concerned with authorization and copyright protection protocol. Paragraph [0076] does not teach or suggest the features of the embodiment of the present invention as recited in claim 1.

Additionally, paragraph [0091] of Kang recites:

“FIG. 10 is an illustration of one protocol format as applied to the practice of the present invention. The format of one protocol for protecting the copyright of digital information to be transmitted by a service server may be arranged with a header that includes information for encrypting the digital information and material that explains the digital information, and an encrypted digital information field. Referring

additionally now to FIG. 5, to understand the structure of the header recall that the digital information requested by the user is encrypted partly by the user key and the temporary validation key so as to prevent replay of the digital information in the absence of the key information, such as when the encrypted digital information is obtained by another entity.”

Again, paragraph [0091] of Kang is teaching prevention of unauthorized access to the digital information and protecting the copyright of the digital information. Paragraph [0091] of Kang also does not teach or suggest the features of the embodiment of the present invention as recited in independent claim 1.

For all of the reasons discussed above, Applicant respectfully submits that claim 1 includes elements that are not taught or suggested by Kang. Thus, claim 1 is patentably distinguishable over Kang. Reconsideration and withdrawal of 35 U.S.C. § 102 rejection of claim 1 is respectfully requested.

Independent claims 21, 34, 40, 48, 62, 73, 90, 100, and 132 recite similar features to independent claim 1. Further, the Examiner cited the same paragraphs in rejecting the features of these independent claims. Therefore, these independent claims are also submitted to be patentably distinguishable over Kang for same reasons as discussed with respect to independent claim 1. Reconsideration and withdrawal of the Section 102 rejection of these claims is respectfully solicited.

Turning now to the rejection of independent claim 108 under 35 U.S.C. § 102(e) as being anticipated by Kang, claim 108 recites:

“decrypting encrypted formatting data associated with information content data;”

The Examiner cited Figure 23B step S555 for rejecting this feature of independent claim 108. Figure 23B step S555 in Kang teaches decrypting an encrypted header. As previously discussed, Kang does not teach or suggest that the header includes formatting data associated with information content data as provided by the embodiment of the present invention as recited in independent claim 108.

Additionally, independent claim 108 recites:

“formatting the associated information content data in one of a plurality of predetermined formats based on the decrypted formatting data, each predetermined format corresponding to a different version of the information

content data for presentation to different receivers or audiences, wherein the information content data is distributable in one form or medium for all audiences or receivers and which version is presented is controlled by entering an appropriate key corresponding to the version for a particular audience or receiver.”

The Examiner cited the same paragraphs (paragraphs [0068], [0076], and [0091]) as discussed with respect to independent claim 1 in rejecting independent claim 108. Applicant respectfully submits that there is no teaching or suggestion in these paragraphs of Kang of the features of independent claim 108 as cited above. Therefore, Applicant respectfully submits that independent claim 108 is patentably distinguishable over Kang, and reconsideration and withdrawal of the 35 U.S.C. § 102 rejection of claim 108 is respectfully solicited.

Independent claim 138 recites similar features to independent claim 108. Therefore, Applicant respectfully submits that independent claim 138 is patentably distinguishable over Kang for the same reasons as discussed with respect to independent claim 108.

Applicant respectfully submits that the secondary references cited in combination with Kang in rejecting some of the dependent claims add nothing to Kang so as to render any of the independent claims discussed herein unpatentable.

As the Examiner’s rejections have been shown to be in clear error and lack essential elements of a *prima facie* anticipation rejection or a *prima facie* obviousness rejection, Applicant respectfully requests that the claims of the present application be allowed to issue.

Respectfully submitted,

Date: October 26, 2007

By: 
Charles L. Moore
Registration No. 33,742
Attorney for Applicants
Moore & Van Allen, PLLC
P.O. Box 13706
Research Triangle Park, NC 27709
Telephone: (919) 286-8000
Facsimile: (919) 286-8199